International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.808.2

(11/2013)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital networks – General aspects

Generic protection switching – Ring protection

Recommendation ITU-T G.808.2

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
General aspects	**G.800–G.809**
Design objectives for digital networks	G.810–G.819
Quality and availability targets	G.820–G.829
Network capabilities and functions	G.830–G.839
SDH network characteristics	G.840–G.849
Management of transport network	G.850-G.859
SDH radio and satellite systems integration	G.860–G.869
Optical transport networks	G.870–G.879
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE –GENERIC AND USER-RELATED ASPECTS	G.1000-G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.808.2

Generic protection switching – Ring protection

Summary

Recommendation ITU-T G.808.2 defines the generic functional models, characteristics and processes associated with various ring protection schemes for connection oriented networks; e.g., optical transport networks (OTNs), synchronous digital hierarchy (SDH) networks. It also defines the objectives and applications for these schemes. The protection scheme described in this Recommendation is shared ring protection.

Generic functional models, characteristics and processes for linear protection and interconnected subnetwork protection schemes are defined in other Recommendations.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.808.2	2013-11-22	15	11.1002/1000/7504-en

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T G.808.2

Generic protection switching – Ring protection

1 Scope

This Recommendation describes the generic aspects of ring protection switching. It covers synchronous digital hierarchy (SDH) and optical transport network (OTN) based protection schemes.

Overviews of ring protection and dual node subnetwork (e.g., dual ring) interconnect schemes will be provided in other Recommendations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.783] Recommendation ITU-T G.783 (2006), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.

[ITU-T G.798] Recommendation ITU-T G.798 (2012), *Characteristics of optical transport network hierarchy equipment functional blocks*.

[ITU-T G.841] Recommendation ITU-T G.841 (1998), *Types and characteristics of SDH network protection architectures*.

[ITU-T G.870] Recommendation ITU-T G.870/Y.1352 (2012), *Terms and definitions for optical transport networks*.

[ITU-T M.495] Recommendation ITU-T M.495 (1988), *Transmission restoration and transmission route diversity: terminology and general principles*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 long path: [ITU-T G.841].

3.1.2 non-revertive (protection) operation: [ITU-T G.870].

3.1.3 protection class: individual: [ITU-T G.870].

3.1.4 revertive (protection) operation: [ITU-T G.870].

3.1.5 ring switching: [ITU-T G.841].

3.1.6 short path: [ITU-T G.841].

3.1.7 span switching: [ITU-T G.841].

3.1.8 steering: [ITU-T G.870].

3.1.9 wrapping: [ITU-T G.870].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 extra traffic: This is the traffic that will be discarded as soon as protection of the normal traffic is required. It will have the lowest availability of the three types of traffic because every protection switch in the ring affects it.

3.2.2 non–pre-emptible unprotected traffic: This is the traffic that will not be affected by the protection switch. It will have availability between that of the Normal traffic and the Extra traffic as it will be affected only by a defect in a section it passes.

3.2.3 normal traffic: This is the traffic that will be protected and will have the highest availability.

3.2.4 ring map: This is a map (table) present in each node on a ring that contains information regarding the order in which the nodes appear on the ring including their node IDs.

NOTE – Also present in each node is a ring circuit map, containing the cross-connection (added, dropped, and passed-through client traffic) maps of all nodes in the ring with the squelch table per node as a subset.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIS	Alarm Indication Signal
APS	Automatic Protection Switching
BER	Bit Error Rate
DEG	Degraded
DLRing	Dedicated section Link Ring
ET	Extra Traffic (signal)
EXER-R	Exercise – Ring
EXER-S	Exercise – Span
FS-R	Forced Switch to protection – Ring
FS-S	Forced Switch to protection – Span
HO	Hold-Off
LOW-R	Lockout of Working channels – Ring switch
LOW-S	Lockout of Working channels – Span switch
LP-S	Lockout of Protection – Span
MS-R	Manual Switch to protection – Ring
MS-S	Manual Switch to protection – Span
NR	No Request
NUT	Non-pre-emptible Unprotected Traffic (signal)
OAM	Operations, Administration and Maintenance
OTN	Optical Transport Network
RR-R	Reverse Request – Ring
RR-S	Reverse Request – Span

SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SD-P	Signal Degrade – Protection
SD-R	Signal Degrade – Ring
SD-S	Signal Degrade – Span
SF	Signal Fail
SF-P	Signal Fail – Protection
SF-R	Signal Fail – Ring
SF-S	Signal Fail – Span
SLRing	Shared section Link Ring protection
SPRing	Shared Protection Ring
SSD	Server Signal Degrade
SSF	Server Signal Fail
TSD	Trail Signal Degrade
TSF	Trail Signal Fail
TT	Trail Termination
WTR	Wait-To-Restore

5 Conventions

No conventions are used.

6 Individual and group protection concept

6.1 Individual protection

In individual protection, the protection mechanism relies on defects detected in the server layer that affect all individual protected entities in the physical section at the same time. In general, individual protection is used in SDH and OTN technologies in physical rings.

6.2 Group protection

In group protection, the protection mechanism relies on defects detected by one of the members of the group or by the whole group in a logical section.

7 Architecture types

The only applicable architecture is a ring. A ring consists of three or more nodes. Each node is connected to two other adjacent nodes in the ring, see Figure 7-1. Two adjacent nodes are connected by a bidirectional span. Each bidirectional span provides in each direction a working entity, a protection entity and, optionally, an entity to transport *non-pre-emptible unprotected traffic* (NUT) signals.

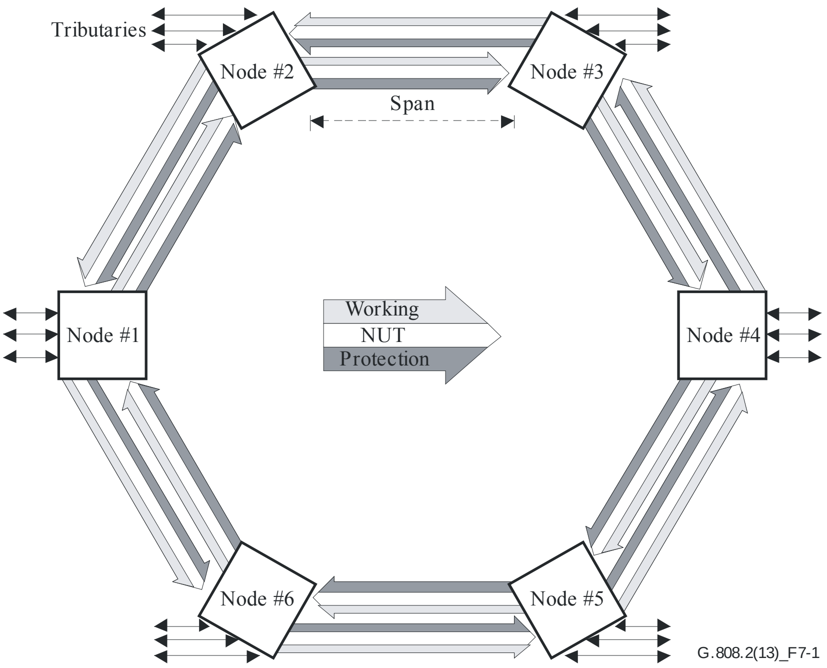

Figure 7-1 – Ring topology

The normal traffic signal transported by the working entity of a section in one direction is protected by the protection entity in the opposite direction of the same section.

The NUT is not protected; it is affected if a section or node it passes through fails.

The protection entity can be used to transport extra traffic signals. Extra traffic signals are not protected; they are affected if any section or node in the ring fails.

7.1 Wrapping protection

The normal traffic signal is wrapped from the working entity to the protection entity in the nodes adjacent to the failed section or node.

During a ring protection switch, normal traffic signal transmitted toward the failed section/node is switched (wrapped) at the node just before the failure to the protection entity in the opposite direction (away from the failure). This bridged traffic signal travels around the ring on the protection entities to the node just after the failure where the normal traffic signal from the protection entity is switched (wrapped) back onto the working entity. In the other direction, the normal traffic signal is bridged and switched in the same manner.

Figure 7-2 illustrates a ring protection switch in response to a section failure.

Since the protection entity of each section (except the failed section) is used for recovery, the protection capacity is effectively shared by all sections.

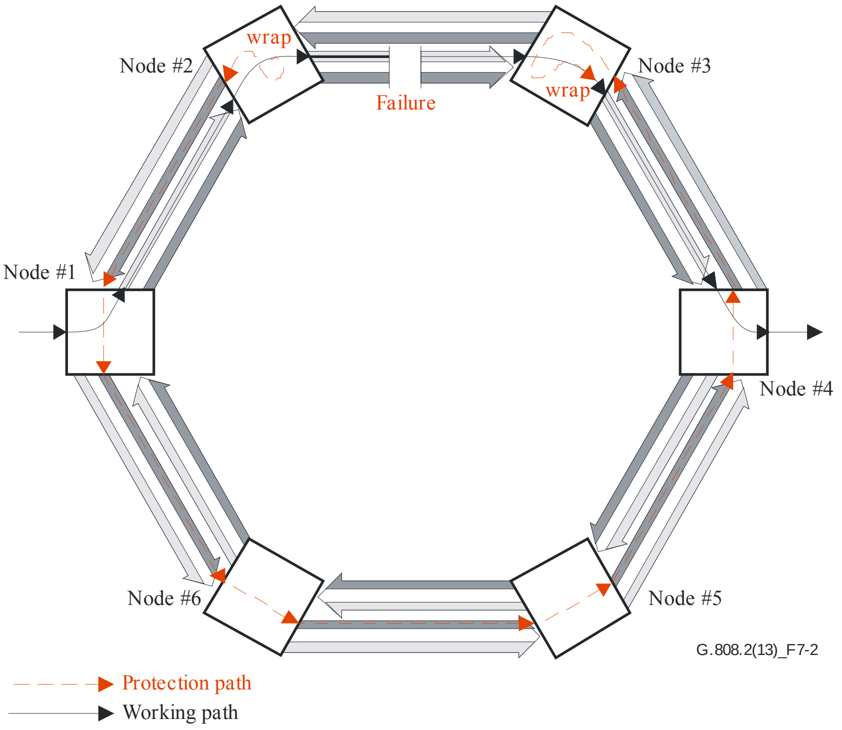

Figure 7-2 – Wrapping

7.2 Steering protection

The normal traffic signal is switched to the protection entity at its ingress and egress nodes.

During a ring protection switch, normal traffic signal transmitted toward the failed section/node is switched (steered) at the node where it enters the ring to the protection entity in the opposite direction (away from the failure). This bridged traffic signal travels around the ring on the protection entities to the node where the normal traffic signal exits the ring and where the normal traffic signal from the protection entity is switched (steered) back to the output. In the other direction, the normal traffic signal is bridged and switched in the same manner.

Figure 7-3 illustrates a ring protection switch in response to a section failure.

Since the protection entity of each section (except the failed section) is used for recovery, the protection capacity is effectively shared by all spans.

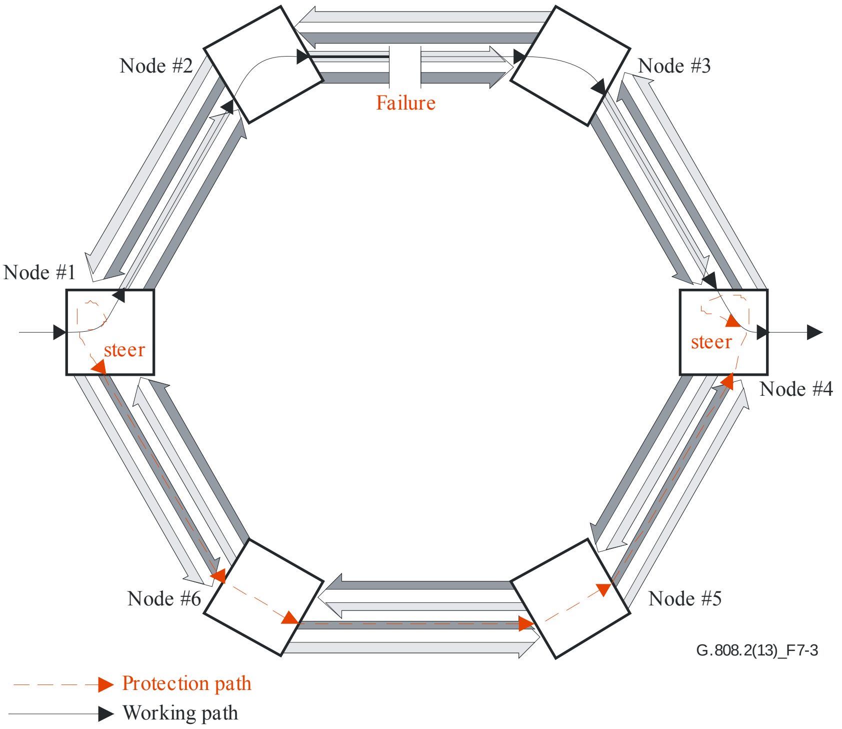

Figure 7-3 – Steering

8 Switching types

- Shared ring protection switching is bidirectional.

9 Operation types

The protection operation types can be a *revertive* operation type or a *non-revertive* operation type.

- In revertive (protection) operation, the normal traffic signal always returns to (or remains on) the working transport entity if the switch requests are terminated. I.e., when the working transport entity has recovered from the defect or the external request is cleared.
- In non-revertive (protection) operation, the normal traffic signal does not return to the working transport entity if the switch requests are terminated.

NOTE – Non-revertive switching is not recommended because the protection entities are shared.

10 Switching protocol

Shared ring protection requires that all nodes in the ring coordinate their actions of bridging and selecting. Therefore, ring nodes communicate with each other via the automatic protection switching (APS) channel.

There are two basic requirements for a protection protocol:

1) The prevention of misconnections.

2) The minimization of the number of communication cycles among the ring nodes in order to minimize the protection switching time.

11 Protection classes and subclasses

The following protection schemes are described:

11.1 Shared section link ring protection (SLRing)

In case fibres are used that carry a shared section link also the term 2-Fibre SPRing is used.

Shared section link ring protection requires only two links for each span of the ring and forms two rings. Each link in the ring carries both working entities and protection entities. On each ring, up to half the entities are defined as working entities and up to half are defined as protection entities, i.e., working entities go around the ring clockwise and anti-clockwise, same for protection entities. The normal traffic carried on working entities is protected by the protection entities travelling in the other ring in the opposite direction (see Figure 11-1). This enables the bidirectional transport of normal traffic.

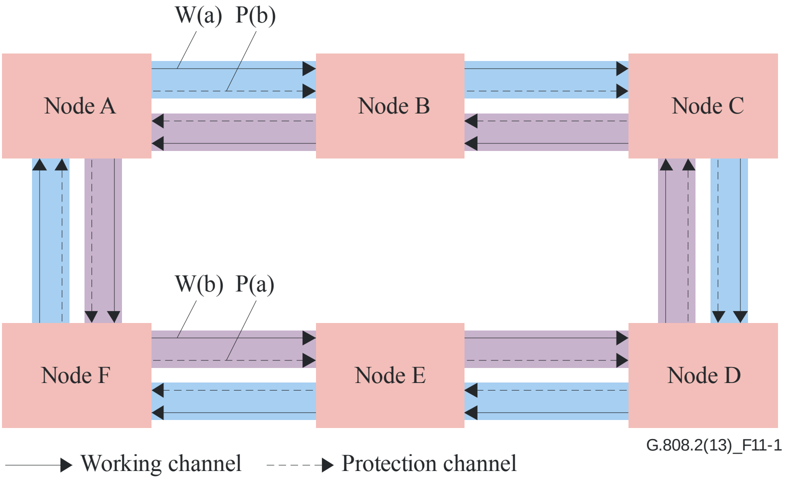

Figure 11-1 – Working entity and protection entity in Shared section Link Ring protection

The normal traffic carried on working entity W(a) is protected by protection entity P(a), and the normal traffic carried on working entity W(b) is protected by protection entity P(b).

11.2 Dedicated section link ring protection (DLRing)

In case fibres are used that carry a dedicated section link also the term 4-Fibre SPRing is used.

Dedicated section link ring protection requires four links for each span of the ring and forms four rings. Working and protection entities are carried over different rings: two rings transmitting in opposite directions carry the working entities; while two rings, also transmitting in opposite directions, carry the protection entities (see Figure 11-2).

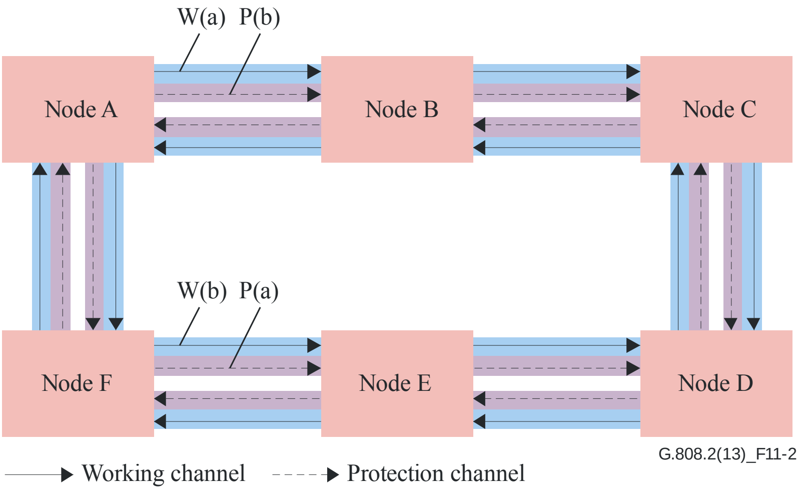

Figure 11-2 – Working entity and protection entity in Dedicated section Link Ring protection

The normal traffic carried on working entity W(a) is protected either by protection entity P(b) in case of span-switch or by protection entity P(a) in case of ring-switch. Similarly, the normal traffic carried on working entity W(b) is protected either by protection entity P(a) in case of span-switch or by protection entity P(b) in case of ring-switch.

11.3 Description

11.3.1 Models for SDH and OTN shared ring protection

Figure 11-3 shows the bidirectional functional model of the connection function of the client layer that is protected by the server layer in each node of a protected ring when no protection switch is activated:

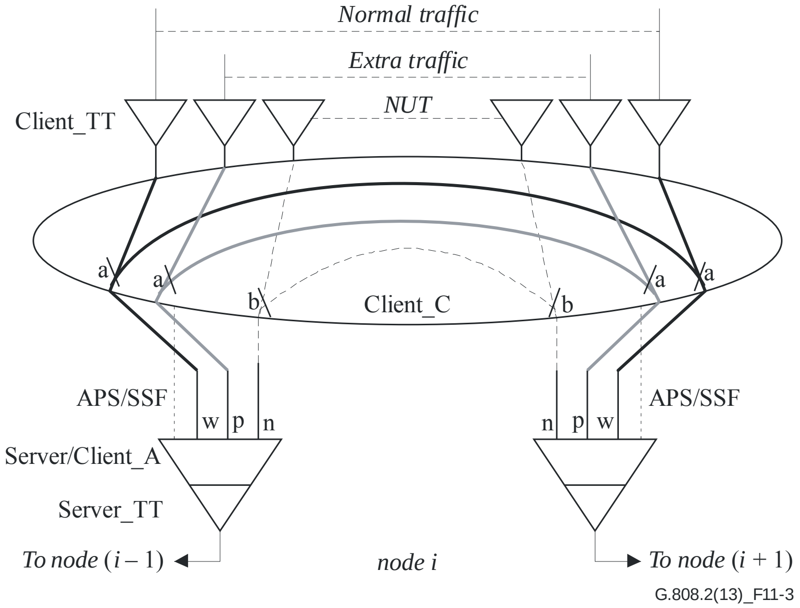

Figure 11-3 – Shared Ring Protection functional model

The following types of traffic will be transported over the section between adjacent nodes:

- **normal traffic**. It is transported in the working entity ('w' in Figure 11-3).
- **extra traffic**. It is transported in the protection entity ('p' in Figure 11-3).

- **non–pre-emptible unprotected traffic** (NUT). It is transported in the NUT entity ('n' in Figure 11-3).

The maximum payload capacity of the working entity is equal to the capacity of the protection entity, as indicated by 'a' in the connection function in Figure 11-3. The payload capacity of the NUT entity is different from the working and protection entity as indicated by 'b' in Figure 11-3. The values 'a' and 'b' are provisioned to have the same value in all nodes of the ring. Note that the 'a' and 'b' entities will carry traffic originating locally or traffic passed through from node (i-1) to node (i+1) and vice versa.

In general, the following limits apply: $1 < a \leq N/2$, $0 \leq b < N$ and $(2a + b) < N$ where N is the total bandwidth capacity of the server section.

11.3.2 Models for wrapping protection on an SLRing

Figure 11-4 shows the functional model in a node adjacent to the failed section or node when ring wrapping protection is activated on a SLRing:

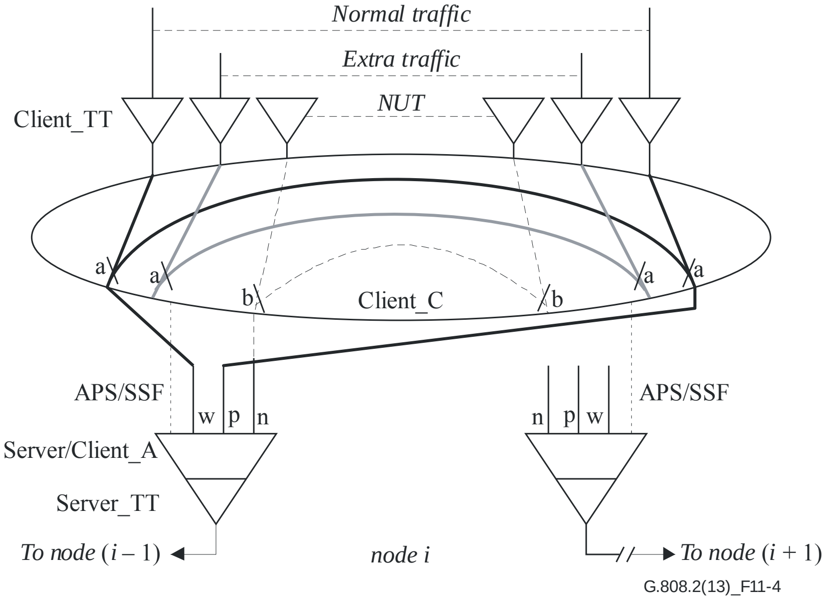

Figure 11-4 – Functional model of a node adjacent to a failure in wrapping protection on a SLRing

Figure 11-5 shows the functional model of an intermediate (non-adjacent) node when ring wrapping protection is activated on a SLRing:

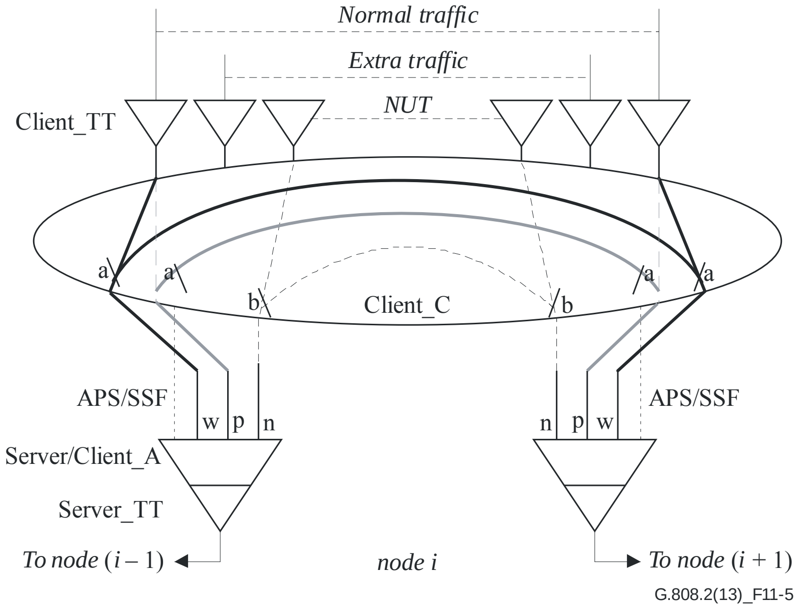

Figure 11-5 – Functional model of an intermediate node in wrapping protection on a SLRing

11.3.3 Models for steering protection on a SLRing

The functional models of the nodes when ring steering protection is activated or for DLRing are for further study.

11.3.4 Models for protection on a DLRing

The functional models of the nodes on a DLRing are for further study.

12 Multi-ring scenario

In actual networks, multi-ring scenarios are widely applied, including tangent rings and intersecting rings (see Figure 12-1). Multi-ring mechanism should inherit and be compatible with the single ring mechanism, to simplify the equipment implementation.

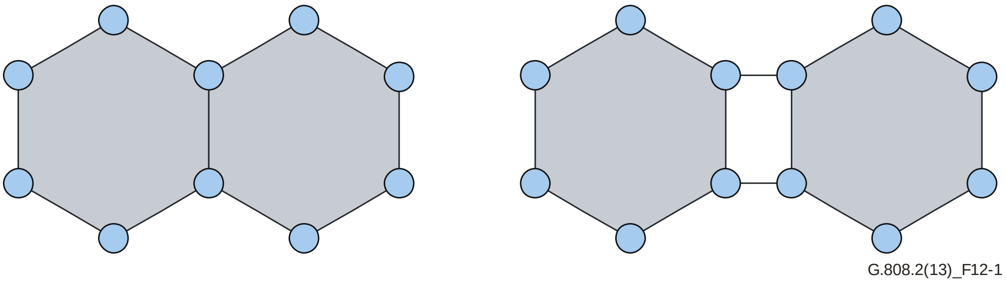

Figure 12-1 – Multiple rings scenario

13 Protection switching performance

The protection switching temporal model derived from [ITU-T M.495] is illustrated in Figure 13-1. Model parameters are defined as follows.

detection time, T_1

Time interval between the occurrence of a network impairment and the detection of a signal fail (SF) or signal degrade (SD) triggered by that network impairment.

hold-off time, T_2:

Time interval after the detection of a SF or SD and its confirmation as a condition requiring the protection switching procedure.

NOTE – Recommendation [ITU-T M.495] identifies time T_2 as the "***waiting time***".

protection switching operations time, T_3:

Time interval between the confirmation of a SF or SD and completion of the processing and transmission of the control signals required to effect protection switching.

protection switching transfer time, T_4:

Time interval between completion of the processing and transmission of the control signals required to effect protection switching and the completion of protection switching operations.

recovery time, T_5:

Time interval between the completion of protection switching operations and the full restoration of protected traffic signal.

NOTE – This may include the verification of switching operations, re-synchronization of digital transmission, etc.

confirmation time, T_c:

The time from the occurrence of the network impairment to the instant when the triggered SF or SD is confirmed as requiring protection switching operations: $T_c = T_1 + T_2$.

transfer time, T_t:

The time interval after the confirmation that a SF or SD requires protection switching operations to the completion of the protection switching operations: $T_t = T_3 + T_4$.

protected traffic signal restoration time, T_r:

The time from the occurrence of the network impairment to the restoration of protected traffic signal:

$T_r = T_1 + T_2 + T_3 + T_4 + T_5 = T_c + T_t + T_5$.

NOTE – An apparent network impairment might be detected by an equipment and not confirmed after confirmation operations. In this case, only times T_1 and T_2 are relevant.

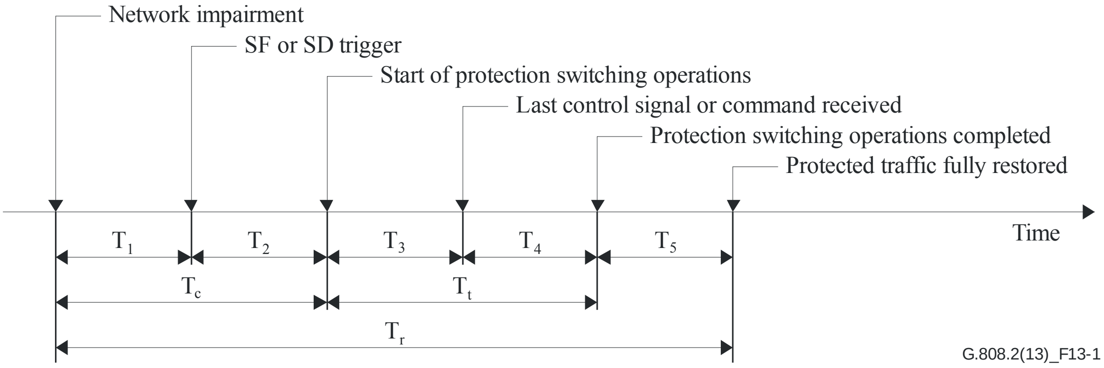
Network impairment
SF or SD trigger
Start of protection switching operations
Last control signal or command received
Protection switching operations completed
Protected traffic fully restored
Time
T1
T2
T3
T4
T5
Tc
Tt
Tr
G.808.2(13)_F13-1

Figure 13-1 – Protection switching temporal model

14 Hold-off timer

Hold-off (HO) timers are intended to operate when a signal is protected by means of nested protection. Those are to allow an inner protection group to restore the traffic signal before the outer protection group tries to do so, in order to limit the number of switch actions.

Each protection selector may have one hold-off timer.

A hold-off timer is started when one or more of the SF or SD conditions in the protection group become active, and runs for a non-resettable period which is provisionable from 0 to 10 seconds in steps of X ms. X is 100 ms (SDH, OTN).

During this period, the modified SF/SD statuses are not passed to the protection switching process.

When the timer expires, the SF/SD status of all signals are read and passed through to the protection switching process. The protection switching process will react on the new SF/SD status at this point.

NOTE 1 – An SF/SD condition does not have to be present for the entire duration of the hold-off period, only the state at the expiry of the hold-off timer is relevant. Further, the SF/SD condition that triggers the hold-off timer does not need to be of the same one as the one at the expiry of the hold-off period.

NOTE 2 – Clearing of SF or SD does not result in a start of the hold-off timer. Instead the wait-to-restore (WTR) timer may be started.

15 Wait-to-restore timer

To prevent frequent operation of the protection switch due to an intermittent defect (e.g., BER fluctuating around the SD threshold), a failed server layer section which carries the working transport entities must become fault-free (e.g., BER less than a restoration threshold). After such a failed server layer section meets this criterion, a fixed period of time shall elapse before normal traffic signals use it again. This period, called wait-to-restore (WTR) period, is of the order of 0…12 minutes and should be capable of being set. An SF or SD condition will override the WTR.

In revertive mode of operation, when the protection is no longer requested, i.e., the failed server layer section which carries the working transport entities is no longer in SD or SF condition (and assuming no other relevant requests exist), a local wait-to-restore state will be activated. Since this state becomes the highest in priority, it is indicated on the APS signal (if applicable), and maintains the normal traffic signal from the previously failed server layer section on their protection transport entities. This state shall normally time out unless any request of higher priority pre-empts this state.

16 Automatic protection switching (APS) signal

An APS signal is used to synchronize the actions at the A and Z ends of the protected domain. Communicated are:

- Request/State Type,
- Source Node ID,
- Destination Node ID,
- Additional Information

The Request/State Type information identifies the highest priority fault condition, external command or protection process state.

The Source and Destination Node ID information when transported in a n-bit field identify:

- **0 ... 2^n-1** Node Identifier (Node ID),

The Additional Information identifies:

- type of request (short/long path),
- signal status (idle, bridged, bridged and switched, …)

The APS signal is transported via the APS channel which is allocated to the server layer section that carries the protection transport entities.

17 Non-pre-emptible unprotected traffic (NUT) and extra traffic (ET)

Non-pre-emptible unprotected traffic is one of three traffic classes in ring protection schemes, the others being normal (protected) traffic and extra traffic. NUT has no protection associated with it, but cannot be dropped from the network to allow protection of other traffic signals.

In circuit-switched networks, extra traffic allows the use of the protection entities for additional traffic signals during normal operation in ring architectures. When a protection switch occurs, this traffic is dropped. Extra traffic provides a cheaper service than either protected traffic or non-pre-emptible unprotected traffic. It is unrelated to the normal traffic signal, coming from a different customer and may be used for example to provide additional capacity in response to a major event.

18 External commands

The autonomous behaviour of the protection switch process on the fault conditions of its transport entities can be modified by means of external (switch) commands. I.e., an external (switch) command issues an appropriate external request on to the protection process.

NOTE – Only one external (switch) command can be issued per side of the protection group. Not accepted or overruled external commands are released/forgotten.

External commands are defined to allow:

1. configuration modifications and maintenance to be performed on the protection group or its transport entities:

   - **Clear**: This command clears the externally initiated command and WTR at the node to which the command was addressed. The node-to-node signalling following removal of the externally initiated commands is performed using the no request (NR) code.

     The following two commands are useful if one span has excessive switching to protection. Another use for these commands includes blocking protection access for some spans that have only traffic that does not need protection. The commands are not time critical (i.e., they do not need to be completed in tens of milliseconds). Thus, they can be transmitted over the management system to each affected node.

   - **Lockout of Working channels – Ring switch (LOW-R)**: This command prevents the normal traffic from working channels over the addressed span from accessing the protection channels for a ring switch by disabling the node's capability to request a ring protection switch of any kind. If any normal traffic is already on protection, the ring bridge is dropped regardless of the condition of the working channels. If no other bridge requests are active on the ring, the NR code is transmitted. This command has no impact on the use of protection channels for any other span. For example, the node can go into any of the pass-through modes.

   - **Lockout of Working channels – Span switch (LOW-S)**: This command prevents the normal traffic from the working channels over the addressed span from accessing the protection channels for a span switch. If any normal traffic is already on protection, the span switch is dropped regardless of the condition of the working channels. If no other bridge requests are active on the ring, the NR code is transmitted. This command has no impact on the use of protection channels for any other span.

   - **Lockout of Protection – Span (LP-S)**: This command prevents the usage of the span for any protection activity and prevents using ring switches anywhere in the ring. If any ring switches exist in the ring, this command causes the switches to drop. If there is a span switch for this span, it is dropped. Thus, all ring switching is prevented (and pre-empted), and span switching is prevented only on the locked-out span.

   - **Forced Switch to protection – Ring (FS-R)**: This command performs the ring switch of normal traffic signal from working entities to the protection entities for the span between the node at which the command is initiated and the adjacent node to which the command is destined. This switch occurs regardless of the state of the protection entities, unless the protection entities are satisfying a higher priority bridge request.

- **Forced Switch to protection – Span (FS-S)**: This command switches the normal traffic signal from the working entities to the protection entities of that span. This switch occurs regardless of the state of the protection entities, unless the protection entities are satisfying a higher priority bridge request, or a signal failure exists on the protection entities of the span.
- **Manual Switch to protection – Ring (MS-R)**: This command performs the ring switch of the normal traffic signal from the working entities to the protection entities for the span between the node at which the command is initiated and the adjacent node to which the command is destined. This occurs if the protection entities are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection entities).
- **Manual Switch to protection – Span (MS-S)**: This command switches the normal traffic signal from the working entities to the protection entities for the same span over which the command is initiated. This occurs if the protection entities are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection entities).

2. testing the protection process and APS channel between the two endpoints:

- **Exercise – Ring (EXER-R)**: This command exercises ring protection switching of the requested channel without completing the actual bridge and switch. The command is issued and the responses are checked, but no normal traffic signal is affected.
- **Exercise – Span (EXER-S)**: This command exercises span protection of the requested channel without completing the actual bridge and switch. The command is issued and the responses are checked, but no normal traffic signal is affected.

19 Automatic commands

The following automatically initiated commands shall be supported:

- **Signal Fail – Span (SF-S)**: An SF is defined as the presence of the trail signal fail (TSF) condition detected on a span. For Dedicated section Link rings, if the failure affects only the working entities, traffic can be restored by switching to the protection entities on the same span. The SF-S bridge request is used to initiate span switching for an SF on the working entities of a Dedicated section Link ring.
- **Signal Fail – Ring (SF-R)**: For Shared section Link rings, all SFs (as defined previously for span switching) are protected using the ring switch. For Dedicated section Link rings, the ring switch is used only if traffic cannot be restored using span switching. If failures exist on both the working and protection entities within a span, it is necessary to initiate a ring bridge request. Hence, this command is used to request ring switching for signal failures. For a dedicated section link ring (DLRing), a SF-R results from the combination of LOW-S and a detected or received working entity failure on the same span or the following combination of detected or received conditions on the working and protection entities:
  - working entity failed AND protection entity failed on the same span;
  - working entity failed AND protection entity degraded on the same span;
  - working entity degraded AND protection entity failed on the same span.
- **Signal Fail – Protection (SF-P)**: This command is used to indicate to an adjacent node that the protection entities are in a Signal Fail state (as defined previously for span switching).

A signal failure of the protection entities is equivalent to a lockout of protection for the span that is affected by the failure. SF-P is used only for Dedicated section Link rings.

- **Signal Degrade – Span (SD-S)**: Signal Degrade is defined as the presence of the TSD condition detected on a span. In Dedicated section Link rings, the working entities on the degraded span can be protected using the protection entities on the same span. This bridge request is used to switch the normal traffic signal to the protection entities in the same span where the failure is located.
- **Signal Degrade – Ring (SD-R)**: For Shared section Link rings, any degraded span is protected using the ring switch (Degradation is defined above under Signal Degrade – Span). For Dedicated section Link rings, a SD-R results from the combination of LOW-S and a detected or received working entity degrade on the same span or the combination of detected or received signal degrade conditions on the working and protection entities on the same span.
- **Signal Degrade – Protection (SD-P)**: This command is used when a node detects a degradation on its protection entities, and there are no higher priority bridge requests existing on the working entities (Degradation is defined above under Signal Degrade – Span). This bridge request is used only for Dedicated section Link rings.
- **Reverse Request – Span (RR-S)**: This command is transmitted to the tail-end node as an acknowledgment for receiving the short-path span bridge request. It is transmitted on the short path only.
- **Reverse Request – Ring (RR-R)**: This command is transmitted to the tail-end node on the short path as an acknowledgment for receiving the short-path ring bridge request.
- **Wait-To-Restore (WTR)**: This command is issued when working entities meet the restoral threshold after an SD or SF condition. It is used to maintain the state during the WTR period unless it is pre-empted by a higher priority bridge request.
- **No Request (NR)**: This command is issued when there is no need to use the protection entities. The protection transport entity carries either no (null) signal or extra traffic signal.

20 Priority

Fault conditions, external commands and protection states are defined to have a relative priority with respect to each other. Priority is applied to these conditions/command/states locally at each node of the ring.

- Lockout of Protection (Span) LP-S
- Signal Fail (Protection) SF-P

  NOTE – In SDH MS-SPRing, LP-S and SF-P share the same priority code. See [ITU-T G.841] for further details.
- Forced Switch (Span) FS-S
- Forced Switch (Ring) FS-R
- Signal Fail (Span) SF-S
- Signal Fail (Ring) SF-R
- Signal Degrade (Protection) SD-P
- Signal Degrade (Span) SD-S
- Signal Degrade (Ring) SD-R
- Manual Switch (Span) MS-S
- Manual Switch (Ring) MS-R
- Wait-To-Restore WTR

- Exerciser (Span) EXER-S
- Exerciser (Ring) EXER-R
- Reverse Request (Span) RR-S
- Reverse Request (Ring) RR-R
- No Request NR

21 SF and SD trigger conditions

An SF condition is a TSF in the server section trail termination function.

TSD in the server section trail termination function is the only SD trigger condition. It is issued on the detection of dDEG. TSD is always local to a Trail Termination function (TT), i.e., it does not pass layer boundaries. The SF and SD conditions are described in the individual equipment specifications.

- For SDH in [ITU-T G.783]
- For OTN in [ITU-T G.798]

22 How to avoid misconnections

22.1 Squelching

In order to perform a ring switch in circuit switching networks, the protection entities are essentially shared among each span of the ring. Extra traffic may reside in the protection entity when the protection entity is not currently being used to restore normal traffic transported on the working entity. Thus, each protection entity is subject to use by multiple services (services from the protection entities on different spans, as well as service from extra traffic). With no extra traffic on the ring, under certain multiple point failures, such as those that cause node(s) isolation, services (from the protection entity on different spans) may contend for access to the same protection entity. This yields a potential for misconnected traffic. With extra traffic on the ring, even under single point failures, normal traffic on the working entity may contend for access to the same protection entity that carries the extra traffic. This also yields a potential for misconnected traffic.

A potential misconnection is determined by identifying the nodes that will act as the switching nodes for a bridge request, and by examining the traffic that will be affected by the switch. The switching nodes can be determined from the node addresses in the APS bytes. The switching nodes determine the traffic affected by the protection switch from the information contained in their ring maps and from the identifications of the switching nodes.

Squelching by inserting the appropriate alarm indication signal (AIS) signal in those entities where misconnected traffic could occur shall avoid potential misconnections. Specifically, the traffic that is sourced or dropped at the node(s) isolated from the ring by the failure shall be squelched. The squelching occurs at the switching nodes and is applied to the normal or extra traffic into or out of the protection entity. I.e., normal traffic into or out of a working entity is never squelched.

22.2 Steering

The avoidance of misconnections for the steering application is for further study.

Bibliography

[b-ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks.*

[b-ITU-T G.842] Recommendation ITU-T G.842 (1997), *Interworking of SDH network protection architectures.*

[b-ITU-T G.873.2] Recommendation ITU-T G.873.2 (2012), *ODUk shared ring protection.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014